ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

A Study on Types of Biometrics Security Systems and Its Applications

Sofia Singh, Rupinder Kaur, Mandeep Kaur

Assistant Professor, PG Department of Computer Science and Applications, GHG Khalsa College Gurusar Sadhar, Ludhiana, Punjab, India.

ABSTRACT: This paper deals with Biometric security systems refers to an automatic recognition of individuals based on a unique features derived from their physiological or behavioral characteristic. These systems are used to conform the individual identity. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. Depending on the context, a biometric system can be either a verification (authentication) system or an identification system. Verification involves confirming or denying a person's claimed identity while in identification, one has to establish a person's identity. Applications of such a system include computer systems security, secure electronic banking, mobile phones, credit cards, secure access to buildings, health and social services. Every medium of authentication has its own advantages and shortcomings. With the increased use of computers as vehicles of information technology, it is necessary to restrict unauthorized access to or fraudulent use of sensitive/personal data. Biometric techniques being potentially able to augment this restriction are enjoying a renewed interest.

KEYWORDS: Fingerprints, Iris, Keystroke, Voice Recognition, Palm Print, Face Recognition.

I. INTRODUCTION

"Biometrics" means "life measurement" but the it is associated with the use of unique physiological characteristics to identify an individual. It is related to biological sciences and consists in the application of statistical methods applied to a wide range of measurable characteristics in biology. It is more commonly related to Information Technology, consisting in electronic identification of human beings based on their physical or behavioral characteristics. A number of biometric traits have been developed and are used to authenticate the person's identity. The idea is to use the special characteristics of a person to identify him. By using special characteristics we mean the using the features such as face, iris, fingerprint, signature.

The method of identification based on biometric characteristics is preferred over traditional passwords and PIN based methods for various reasons such as:

- The person to be identified is required to be physically present at the time-of-identification.
- The need to remember a password or carry a token.

A biometrics system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic".

A biometric system can be either an 'identification' system or a 'verification' system, which are defined below in Fig 1.

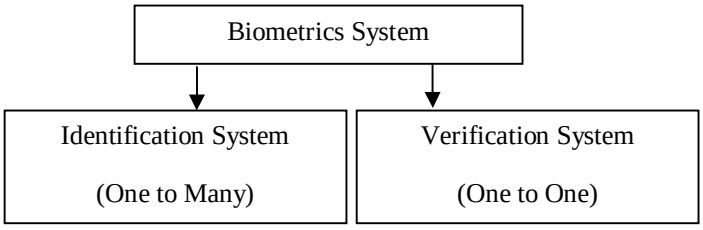

Fig. 1 Biometrics system

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

- **Identification -** Identifying an individual based upon comparison of biometrics collected against a database of previously collected samples. Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning someone in crowd with a camera and using face recognition technology, one can determine matches against a known database.
- **Verification -** Verifying that an individual is the person that they claim to be, based upon validating a sample collected against a previously collected biometric sample for the individual. Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan.

II. DESIGN OF BIOMETRICS SYSTEM

Biometrics authentication requires comparing an enrolled biometric sample against a newly captured biometric sample i.e. captured during a login. This is a three-step process includes Capture, Process and Enroll that is followed by a Verification or Identification process which is discussed in fig 2 and3.

- During Capture process, raw biometric data is captured by a sensing device such as a fingerprint scanner or video camera.
- The second phase of processing is to extract the distinguishing characteristics from the raw biometric sample and convert into a processed biometric identifier record or biometric sample or biometric template.
- Next phase does the process of enrollment. Here the processed sample i.e. a mathematical representation of the biometric - not the original biometric sample is stored / registered in a storage medium for future comparison during an authentication.

A biometric system can be classified into two modules-

(i) **Database Preparation Module:** The Database Preparation Module consists of two sub-modules, and they are (a) Enroll Module and (b) Training Module while the other module

(ii) **Verification Module:** Verification module can be divided into two modules (a) Matching Module and (b) Decision Module.

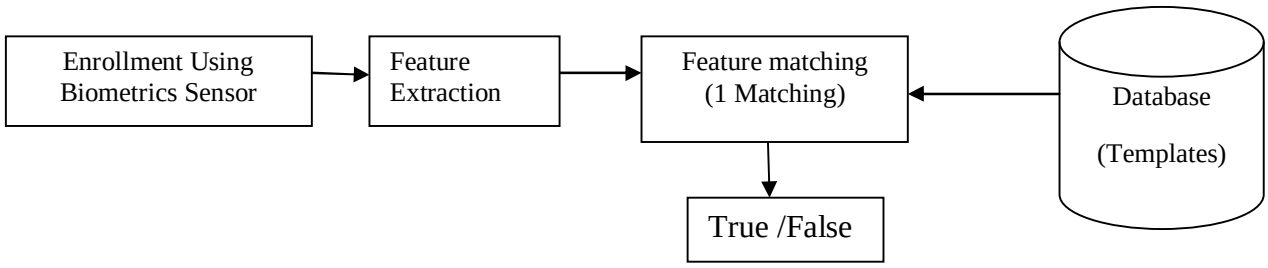

Fig.2 Verification system (One to One)

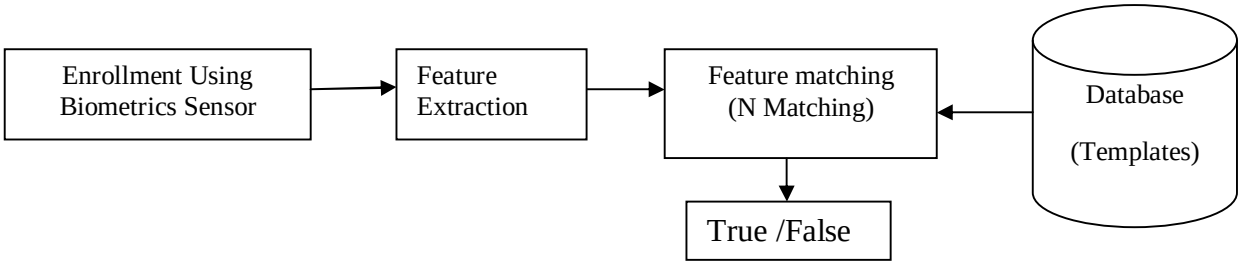

Fig.3 Identification System (One to Many)

Data captured for biometric process should have following characteristics:-

1. **Invariance of properties:** They should be constant over a long period of time. It should not be changed over time. The attribute should not be subject to significant differences based on age either episodic or chronic disease.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

2. **Unique:** Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye color are all attributes that are unique assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.
3. **Reducibility:** The captured data should be capable of being reduced to a file which is easy to handle.
4. **Reliable:** The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.
5. **Comparable:** Should be able to reduce the attribute to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.
6. **Inimitable:** The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

III. TYPES OF BIOMETRICS SYSTEM

All biometrics identifiers can be divided into two big groups shown in fig 4: 1) Physiological 2) Behavioral

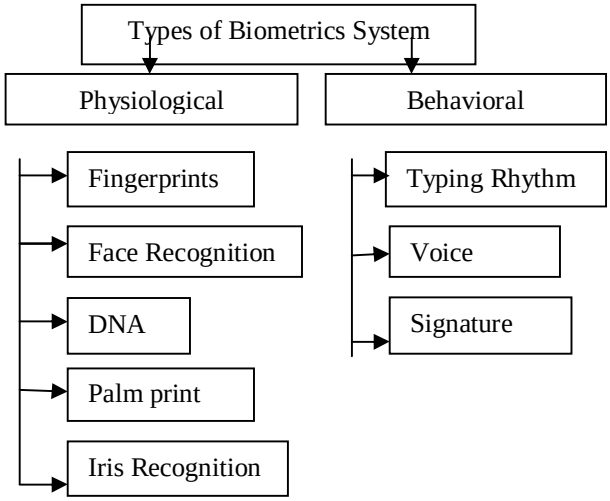

Fig.4 Types of Biometrics System

IV. PHYSIOLOGICAL TYPE OF BIOMETRICS

Physiological systems are considered to be more reliable as individual features of a person that are used by these systems do not change by influence of psycho emotional state. Physiological systems of identification deal with statistical characteristics of a person: fingerprints, iris recognition, hand geometry, DNA, face recognition, palm print.

- **Fingerprints:** Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. Fingerprints are considered nowadays one of the most reliable biometric characteristic for human recognition due to their individuality and persistence. Furthermore, fingerprint-based authentication is traditionally associated with criminal-authentication methods. State-of-the-art authentication methods have demonstrated adequate accuracies for fingerprint recognition methods, however, for the sake of human identification there are still some open tasks. First, the processing time of the current algorithms should be reduced since the output of such systems should be done in real time. Second, the non-controlled interaction between users and capture devices will produce misaligned and rotated images. Fingerprint verification may be a good choice for in-house systems, where you can give users adequate explanation and training, and where the system operates in a controlled environment. It is not surprising that the workstation access application area seems to be based almost exclusively on fingerprints, due to the relatively low cost, small size, and ease of integration of fingerprint authentication devices.
- **Face Recognition:** Face recognition analyzes facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. Each person around the world has a distinctly unique face, even two twins

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

that the human eye cannot tell apart. It may be something as small as the slightly different placing of the eyebrows, the width of the eyes, or the breadth of the nose. There are certain markers that enable these biometric recognition scanners to instantly identify the uniqueness of each person scanning their facial features, thus enabling the device to ensure that only the single person with the correct bone structure and feature placement can gain access. The face recognition process often involves three different steps: (1) detect whether there exists a face in an image, (2) locate the face and (3) recognize the face. For each of the three mentioned steps, there are some challenges to be considered. First, face images are captured under non-controlled conditions. Therefore, these images may be characterized by the presence of different illumination conditions and backgrounds. Furthermore, changes in the facial expressions and occlusions of some facial features may reduce the overall recognition accuracy. Due to these aspects face recognition is a challenging research field.

- **DNA:** DNA stands for Deoxyribonucleic Acid and is a molecule that contains biological instructions of the living organisms. The DNA is composed of chemical building blocks called nucleotides. A sequence of DNA that contains information for producing a protein is known as gene, whereas the whole DNA instructions of the organisms are called genome. The human genome is shared about 99.5% to 99.9% across the human beings, however, even the small percentages of difference are of the order of millions of base pairs. The human genome is unique to each individual; however this affirmation is not valid for identical twins since they share the same DNA patterns. The low degree of popularity of this biometric characteristic is based on three factors: (1) privacy concerns, some additional information of the individual could be obtained such as diseases, (2) real-time authentication capabilities, this technique involves high computational resources and is difficult to be automatized since it requires some chemical processes, and (3) access availability, it is easy to steal a piece of DNA from an individual and this information could be therefore used for fraudulent purposes
- **Palm print:** This biometric offer a good balances of performance characteristics and is relatively easy to use. It might be suitable where there are more users or where users access the system infrequently and are perhaps less disciplined in their approach to the system. When you place your hand on a scanner, you not only have a unique fingerprint pattern, but the size and shape of your entire hand is also very unique. This includes the width and length of your palm, the width and length of your fingers, the distance between each knuckle, and the depth of each of the lines in your palm. This is more complex than regular fingerprint scanning, and will be much more accurate with less chance of falsification. Some of these products will be far costlier than the others, as they feature technology that is much more complex. However, the amount that you spend on the various types of biometric devices will be directly proportionate to the level of security you need. The more secure you want your home or business to be, the more costly your device will be.
- **Iris Recognition:** It scan the unique biometric pattern in each person's iris, and match it against a certain number of unique identifying marks that set every person apart from everyone else. Iris scanning and retinal scanning are both used to identify a person according to their unique pattern, but they tend to be far costlier and more complex. Iris based biometric, on the other hand, involves analyzing features found in the colored ring of tissue that surrounds the pupil. Iris scanning, undoubtedly the less intrusive of the eye-related biometrics, uses a fairly conventional camera element and requires no close contact between the user and the reader. In addition, it has the potential for higher than average template-matching performance. Iris biometrics work with glasses in place and is one of the few devices that can work well in identification mode. Its visual texture information is formed during the fetal period and its formation is extended up to the two first years of life. Iris-based authentication methods take into advantage the facts that the iris information is unique across individuals, and its main characteristics do not change over time, as is the case of fingerprints. Besides its main properties, the texture of the iris is believed to be very difficult to be modified surgically. Ease of use and system integration has not traditionally been strong points with iris scanning devices, but you can expect improvements in these areas as new products emerge.

V. BEHAVIORAL TYPE OF BIOMETRICS

Behavior methods of identification pay attention to the actions of a person, giving the user an opportunity to control his actions. Biometrics based on these methods takes into consideration high level of inner variants (mood, health condition, etc), that is why such methods are useful only in constant use. Behavior or sometimes called psycho-logical characteristics such as voice, gait, typing rhythm are influenced on psychological factors.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

- **Typing Rhythm:** Nowadays, our world is fully computerized. Almost every house has so important part of the world. Computer is used not only for work, but also for entertainment, communication, education and so on. Keyboard- is an inalienable part of computer. It can be a separate device, or attached inside the laptop or smart phone. Keyboard- is the part that helps us to communicate with computer. People use keyboard in different ways. Some people type fast, some slow. The speed of the typing also depends on the mood of a person and a time of a day. Biometric keystroke recognition – is a technology of recognizing people from the way they are typing. It is rather important to understand that this technology does not deal with "what" is written but "how" it is written. Keystroke recognition is considered to be a natural choice for computer login and network security. The main features that are used to describe typing pattern of a user are:

  - Latencies Between Successive Keystrokes
  - Finger Placement
  - Pressure applied on keys
  - Overall typing speed

- **Voice**: Every person in the world has a unique voice pattern, even though the changes are slight and barely noticeable to the human ear. However, with special voice recognition software, those tiny differences in each person's voice can be noted, tested, and authenticated to only allow access to the person that has the right tone, pitch, and volume of voice. It can be surprisingly effective at differentiating two people who have almost identical voice patterns. Voice is a combination of physical and behavioral characteristics that are related to the voice signal patterns of a given individual. The physical characteristics of voice are related to the appendages that form its sound. These characteristics include for example, the vocal tracts, mouth, nasal cavities, and lips. On the other hand, the behavioral characteristics of voice are related to the emotional and physical states of the speaker. Voice-based authentication methods have to face some challenges related for example to the room acoustics, misspoken phrases or individuals emotional states. Due to all of these problems, this technique is not adequate for large-scale systems
- **Signature:** Signature verification analyzes the way a user signs her name. Signing features such as speed, velocity, and pressure are as important as the finished signature's static shape. Signature verification enjoys a synergy with existing processes that other biometrics do not. People are used to signatures as a means of transaction-related identity verification, and most would see nothing unusual in extending this to encompass biometrics**.** The handwriting of a given individual can be thought as representing his/her own characteristics. Signatures have been widely used in different areas ranging from government and legal applications to commercial ones. Traditionally, signature authentication may be either static or dynamic. Static signature authentication uses only the geometric features of the signatures, whereas the dynamic authentication uses not only those features, but also some additional information such as velocity, acceleration, pressure, and trajectory of the signatures. Furthermore, although it has proven reasonable authentication accuracy, it is not high enough for large-scale applications.

VI. APPLICATION OF BIOMETRICS SYSTEM

There are various fields in which biometrics system are used:

- **Military programs**- the military has long been interested in biometrics and the technology has enjoyed extensive support from the national security community.
- **Surveillance -** using cameras one can monitor the very busy places such as stadiums, airports, meetings, etc. Looking in the crowds for suspect, based on the face recognition biometric, using a images (e.g., mug shots) database of wanted persons or criminals.
- **Account access -** The use of biometric for the access to the account in the bank allows keeping definitive and auditable records of account access by employees and customers. Using biometry the customers can access accounts and employees can log into their workstations.
- **ATMs -** the use of biometric in the ATM transaction allows more security. A more receptive market for biometrics may be special purpose kiosks, using biometric verification to allow a greater variety of financial transaction than are currently available though standard ATMs.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

- **Online banking -** Internet based account access is already widely used in many places, the inclusion of biometric will make more secure this type of transactions from home. Currently, there are many pilot programs using biometric in home banking.
- **PC/Network access -** The use of biometric log-in to local PCs or remotely through network increase the security of the overall system keeping more protected the valuable information.
- **E-commerce -** biometric e-commerce is the use of biometrics to verify of identity of the individual conduction remote transaction for goods or services
- **Time and attendance monitoring -** In this sector the biometrics is used for controlling the presence of the individuals in a determine area. For example for controlling the time sheet of the employees or the presence of students at the classroom
- **Access to personal information -** Using biometrics, the medical patient information maybe stored on smart card or secures networks; this will enable the access of the patients to their personal information.
- **Air travel -** In many airport are already used a biometric system in order to reduce the inspection processing time for authorized travelers.
- **Border crossing -** The use of biometrics to control the travelers crossing the national or state border is increasing, especially in regions with high volume of travelers or illegal immigrants.
- **Passports -** Some country already issues passports with biometric information on a barcode or smart chips. The use of biometrics prevents the emission of multiple passports for the same person and also facilitates the identification at the airports and border controls.

VII. CONCLUSION

In this we discussed about Biometrics System design which includes verification and identification systems. Further we considered the types of biometrics system which includes physiological and behavioral biometrics systems. Physiological includes various techniques such as fingerprint scan, face, iris recognition, palm prints where as behavioral includes typing speed, voice recognition, signature recognition system. At last give attention on various applications of biometrics system.

REFERENCES

[1] Woodward, J. D., Orlans, N. M., & Higgins, P. T. (2003). Biometrics. New York: McGraw-Hill/Osborne.
[2] Ashbourn, J. (2000). Biometrics: Advanced identity verification: The complete guide. London: Springer.
[3] Biometrics: Personal identification in networked society. (2013). Place of publication not identified: Springer-Verlag New York.
[4] Fleming, S. (2007). Biometrics. Oxford: Oxford University Press.
[5] Newman, R. C. (2009). Biometrics: Application, technology, and management. Clifton Park, NY: Delmar.
[6] Nichols, E. R. (2011). Biometrics: Theory, applications, and issues. New York: Nova Science.
[7] Reid, P. (2003). Biometrics and Network security. Upper Saddle River, NJ: Prentice Hall PTR.
[8] Traore, I., & Ahmed, A. A. (2012). Continuous authentication using biometrics: Data, models, and metrics. Hershey, PA: Information Science Reference.
[9] Yang, J., & Poh, N. (2011). Recent application in biometrics. Rijeka: InTech.

BIOGRAPHY

Sofia Singh is a Assistant Professor in the PG Department of Computer Science and Applications, GHG Khalsa College Gurusar Sadhar, Ludhiana, Punjab, India. She received Master of Science in Information Technology (MSc IT)degree in 2013 from Panjab University , Chandigarh , India. Her research interests are Graphics, Artificial Intelligence and Algorithms etc.

Rupinder Kaur is a Assistant Professor in the PG Department of Computer Science and Applications, GHG Khalsa College Gurusar Sadhar, Ludhiana, Punjab, India. She received Master of Science in Information Technology (MSc IT)degree in 2014 from Panjab University , Chandigarh , India. Her research interests are Computing Software, Operational Research, Operating System, E-Commerce, Web Applications etc.

Mandeep Kaur is a Assistant Professor in the PG Department of Computer Science and Applications, GHG Khalsa College Gurusar Sadhar, Ludhiana, Punjab, India. She received Master of Science in Information Technology (MSc IT)degree in 2012 from Panjab University , Chandigarh , India. Her research interests are Web Applications, Java, DBMS etc.